SCIENCE CHINA
Mathematics

• ARTICLES •

July 2013 Vol. 56 No. 7: 1403–1412
doi: 10.1007/s11425-013-4668-z

Binary cyclic codes with two primitive nonzeros

FENG Tao[1], LEUNG KaHin[2] & XIANG Qing[3,*]

[1] *Department of Mathematical Sciences, Zhejiang University, Hangzhou* 310027*, China;*
[2] *Department of Mathematical Sciences, National University of Singapore, Kent Ridge* 119260*, Singapore;*
[3] *Department of Mathematical Sciences, University of Delaware, Newark, DE* 19716*, USA*
Email: tfeng@zju.edu.cn, matkhl@nus.edu.sg, xiang@math.udel.edu

Received January 21, 2013; accepted June 3, 2013; published online June 14, 2013

Abstract In this paper, we make some progress towards a well-known conjecture on the minimum weights of binary cyclic codes with two primitive nonzeros. We also determine the Walsh spectrum of $\mathrm{Tr}(x^d)$ over $\mathbb{F}_{2^m}$ in the case where $m = 2t$, $d = 3 + 2^{t+1}$ and $\gcd(d, 2^m - 1) = 1$.

Keywords cyclic code, minimum weight, Walsh spectrum

MSC(2010) 11T71, 94B15

Citation: Feng T, Leung K H, Xiang Q. Binary cyclic codes with two primitive nonzeros. Sci China Math, 2013, 56: 1403–1412, doi: 10.1007/s11425-013-4668-z

1 Introduction

In this paper, we are concerned with the weight distributions of binary cyclic codes with two primitive nonzeros. Let $q = 2^m$, where $m \geqslant 1$ is an integer, and $\mathbb{F} = \mathbb{F}_q$, the finite field of size q. Let α be a primitive element of $\mathbb{F}$, and $\mathcal{C}_d$ be the binary cyclic code of length $q-1$ with two nonzeros α^{-1} and α^{-d}, where d is an integer such that $1 \leqslant d \leqslant q-2$, $\gcd(d, q-1) = 1$. Then $\mathcal{C}_d$ is a $[q-1, 2m]_2$ code, and its codewords are given by

$$c(a,b) = (\mathrm{Tr}(a+b), \mathrm{Tr}(a\alpha^d + b\alpha), \ldots, \mathrm{Tr}(a\alpha^{(q-2)d} + b\alpha^{q-2})), \quad a, b \in \mathbb{F},$$

where Tr is the absolute trace function defined on $\mathbb{F}$.

Let us consider the Hamming weights of $c(a,b)$, where $a, b \in \mathbb{F}$. When exactly one of a, b is 0, the codeword $c(a,b)$ has weight $q/2$. When a, b are both nonzero, $c(a,b)$ has weight

$$\frac{1}{2}\sum_{i=0}^{q-2}(1 - (-1)^{\mathrm{Tr}(a\alpha^{di} + b\alpha^i)}) = \frac{1}{2}\left(q - \sum_{x\in\mathbb{F}}(-1)^{\mathrm{Tr}(x^d + ba^{-\frac{1}{d}}x)}\right), \tag{1.1}$$

where we use $1/d$ to denote the unique integer j such that $jd \equiv 1 \pmod{q-1}$ and $1 \leqslant j \leqslant q-2$. Therefore, the weight distribution of $\mathcal{C}_d$ is completely determined by the Walsh spectrum of the function $f_d : \mathbb{F} \to \mathbb{F}_2$, $x \mapsto \mathrm{Tr}(x^d)$, and vice versa. Here *the Walsh coefficients* of f_d are defined by

$$W_d(a) = \sum_{x\in\mathbb{F}}(-1)^{\mathrm{Tr}(x^d + ax)}, \quad a \in \mathbb{F}.$$

*Corresponding author

The distribution of $W_d(a), a \in \mathbb{F}$, is called *the Walsh spectrum* of f_d. The problem of determining the Walsh spectrum of f_d is also equivalent to the problem of determining the crosscorrelations of an m-sequence and its d-decimation. We refer the reader to the appendix in [9] for more details on various formulations of this problem. A lot of work has been done on determining the Walsh spectrum of f_d when d takes special forms, see [2, 4, 8, 11]. There are a few general conjectures on the Walsh spectrum of f_d, which have proved to be quite challenging. We refer the reader to the recent paper [1] for a list of these conjectures, and some recent progress made on them.

In this paper, we are primarily interested in the following well-known conjecture due to Sarwate [1]; see [3, p. 258] also.

Conjecture 1.1. Let $m = 2t$, and $\mathcal{C}_d$ be the $[2^m - 1, 2m]$ binary cyclic code with two nonzeros α^{-1} and α^{-d} $(\gcd(d, 2^m - 1) = 1)$, where α is a primitive element of $\mathbb{F}$. Then the minimum distance of $\mathcal{C}_d \leqslant 2^{m-1} - 2^t$.

Using (1.1), the existence of a nonzero codeword of weight $\leqslant 2^{m-1} - 2^t$ is equivalent to the existence of a nonzero $a \in \mathbb{F}$ such that $W_d(a) \geqslant 2^{t+1}$. Charpin [3] showed that Conjecture 1.1 is true when $d \equiv 2^j \pmod{2^t - 1}$, for some j, $0 \leqslant j \leqslant t-1$. (Such d's are called the Niho exponents.)

In this paper, without putting any conditions on d (of course, $\gcd(d, 2^m - 1) = 1$ is still assumed), we shall prove an upper bound on the minimum distance of $\mathcal{C}_d$, which is slightly weaker than the bound in Conjecture 1.1. Furthermore, we will determine the weight distributions of $\mathcal{C}_d$ for two special classes of d; one of the two classes was previously considered by Cusick and Dobbertin [4], the other class is new. Details are given in Section 3. Throughout the rest of this paper, we shall fix $m = 2t$, and use Tr_m, Tr_t to denote the absolute traces defined on $\mathbb{F}$ and $\mathbb{F}_{2^t}$, respectively. Also we use $\mathrm{Tr}_{m/t}$ (resp. $\mathrm{N}_{m/t}$) to denote the relative trace (resp. norm) from $\mathbb{F}$ to $\mathbb{F}_{2^t}$. We shall drop the subscripts if we believe that no confusion will arise.

2 An upper bound on the minimum weight of $\mathcal{C}_d$

First, we give a summary of some well-known identities involving the Walsh coefficients $W_d(a)$, $a \in \mathbb{F}$. We refer the reader to [3, 6, 7, 9] for the proof of these identities.

Lemma 2.1. (1) $\sum_{a\in\mathbb{F}} W_d(a) = q$, $\sum_{a\in\mathbb{F}} W_d(a)^2 = q^2$.

(2)

$$\sum_{a\in\mathbb{F}_{2^t}} W_d(au) = \begin{cases} q, & \text{if } u \in \mathbb{F}_{2^t}^*, \\ 0, & \text{if } u \notin \mathbb{F}_{2^t}. \end{cases}$$

Now, we are ready to prove our first result.

Theorem 2.1. *Let $m = 2t$, and $\mathcal{C}_d$ be the $[2^m - 1, 2m]$ binary cyclic code with two nonzeros α^{-1} and α^{-d} $(\gcd(d, 2^m - 1) = 1)$, where α is a primitive element of $\mathbb{F}$. Then the minimum distance of $\mathcal{C}_d < 2^{m-1} - 2^{t-1} - 2^{\lfloor t/2\rfloor - 1}$; in other words, there is a nonzero $a \in \mathbb{F}$ such that $W_d(a) > 2^t + 2^{\lfloor t/2\rfloor}$.*

Proof. For any nonzero $b \in \mathbb{F} \setminus \mathbb{F}_{2^t}$, by direct calculations we have

$$\sum_{a\in\mathbb{F}_{2^t}} W_d(a)(1 - (-1)^{\mathrm{Tr}_m(ba)}\epsilon_b) = 2^m + 2^t|M_b|, \tag{2.1}$$

where $M_b = \sum_{x\in\mathbb{F}_{2^t}} (-1)^{\mathrm{Tr}_m((x+b)^d)}$ and $\epsilon_b = \pm 1$ is chosen such that $\epsilon_b M_b = -|M_b|$. For each $b \in \mathbb{F} \setminus \mathbb{F}_{2^t}$, it will be convenient to introduce a function p_b on $\mathbb{F}_{2^t}$ defined by

$$p_b(a) := 1 - (-1)^{\mathrm{Tr}_m(ba)}\epsilon_b, \quad \forall\, a \in \mathbb{F}_{2^t}.$$

Then for $b \in \mathbb{F} \setminus \mathbb{F}_{2^t}$, we have $\sum_{a\in\mathbb{F}_{2^t}} p_b(a) = 2^t$, $p_b(a) \geqslant 0$, and (2.1) can be rewritten as

$$\sum_{a\in\mathbb{F}_{2^t}} W_d(a)p_b(a) = 2^m + 2^t|M_b|. \tag{2.2}$$

Next we compute

$$\begin{aligned}\sum_{b\in\mathbb{F}} M_b^2 &= 2^t \sum_{b\in\mathbb{F}}\sum_{x\in\mathbb{F}_{2^t}} (-1)^{\mathrm{Tr}_m((x+b)^d+b^d)}\\ &= 2^t|\mathbb{F}| + 2^t \sum_{b\in\mathbb{F}}\sum_{x\in\mathbb{F}_{2^t}^*} (-1)^{\mathrm{Tr}_m(x^d((1+b)^d+b^d))}\\ &= 2^t|\mathbb{F}| + 2^t(2^t\cdot|\{b\in\mathbb{F}\mid \mathrm{Tr}_{m/t}((1+b)^d+b^d)=0\}| - |\mathbb{F}|)\\ &= 2^{2t}|\{b\in\mathbb{F}\mid (1+b)^d+b^d\in\mathbb{F}_{2^t}\}|.\end{aligned}$$

Since $M_b = 2^t$ if $b\in\mathbb{F}_{2^t}$, we thus have

$$\sum_{b\in\mathbb{F}\setminus\mathbb{F}_{2^t}} M_b^2 = 2^{2t}\cdot|\{b\in\mathbb{F}\setminus\mathbb{F}_{2^t}\mid (1+b)^d+b^d\in\mathbb{F}_{2^t}\}|.$$

Let $c\in\mathbb{F}^*$ be an element of order 2^t+1. Then a system of coset representatives of $(\mathbb{F}_{2^t},+)$ in $(\mathbb{F},+)$ is given by uc, $u\in\mathbb{F}_{2^t}$. Since $M_{b+x}=M_b$ for any $x\in\mathbb{F}_{2^t}$, and $\mathbb{F}\setminus\mathbb{F}_{2^t} = \bigcup_{u\in\mathbb{F}_{2^t}^*}(uc+\mathbb{F}_{2^t})$, we get

$$\sum_{u\in\mathbb{F}_{2^t}^*} M_{uc}^2 = 2^t\cdot|\{b\in\mathbb{F}\setminus\mathbb{F}_{2^t}\mid (1+b)^d+b^d\in\mathbb{F}_{2^t}\}|. \tag{2.3}$$

If $u\in\mathbb{F}_{2^t}^*$, then we have

$$M_{uc} = \sum_{x\in\mathbb{F}_{2^t}} (-1)^{\mathrm{Tr}_m((x+uc)^d)} = \sum_{x\in\mathbb{F}_{2^t}} (-1)^{\mathrm{Tr}_t(u^d((x+c)^d+(x+c^{2^t})^d))} = \sum_{z\in R_d}\psi_{u^d}(z),$$

where R_d denotes the multiset "$(x+c)^d+(x+c^{2^t})^d$, $x\in\mathbb{F}_{2^t}$" (each element of R_d indeed belongs to $\mathbb{F}_{2^t}$), and ψ_{u^d} is the additive character of $\mathbb{F}_{2^t}$ defined by

$$\psi_{u^d}(x) = (-1)^{\mathrm{Tr}_t(u^d x)}, \quad x\in\mathbb{F}_{2^t}.$$

We write the multiset R_d as a group ring element, $R_d=\sum_{g\in\mathbb{F}_{2^t}} r_g[g]\in\mathbb{Q}[(\mathbb{F}_{2^t},+)]$. Then $\sum_{g\in\mathbb{F}_{2^t}} r_g=2^t$, each r_g is a nonnegative integer, and for $u\in\mathbb{F}_{2^t}^*$, $M_{uc}=\psi_{u^d}(R_d)$. Furthermore, note that each coefficient r_g of R_d must be even since $(x+c)^d+(x+c^{2^t})^d = ((x+c+c^{2^t})+c)^d+((x+c+c^{2^t})+c^{2^t})^d$ for any $x\in\mathbb{F}_{2^t}$, and $c+c^{2^t}\neq 0$. We compute the coefficient of the identity (i.e., the zero element of $\mathbb{F}_{2^t}$) in $R_dR_d^{(-1)}$ in two ways, where $R_d^{(-1)}=\sum_{g\in\mathbb{F}_{2^t}} r_g[-g]$. In fact, we have $R_d^{(-1)}=R_d$ here since the characteristic of $\mathbb{F}_{2^t}$ is 2. On the one hand, this coefficient is equal to

$$\sum_{g\in\mathbb{F}_{2^t}} r_g^2 \geqslant 2^2\cdot 2^{t-1} = 2^{t+1}.$$

On the other hand, by the inversion formula (see, for example, [6]), the coefficient of the identity element in $R_dR_d^{(-1)}$ is equal to $\frac{1}{2^t}\sum_{u\in\mathbb{F}_{2^t}}\psi_{u^d}(R_d)^2 = \frac{1}{2^t}\sum_{u\in\mathbb{F}_{2^t}} M_{uc}^2$. It follows that

$$\sum_{u\in\mathbb{F}_{2^t}} M_{uc}^2 \geqslant 2^{2t+1}.$$

Using (2.3) we now obtain

$$(2^t)^2 + 2^t\cdot|\{b\in\mathbb{F}\setminus\mathbb{F}_{2^t}\mid (1+b)^d+b^d\in\mathbb{F}_{2^t}\}| \geqslant 2^{2t+1}.$$

Therefore,

$$|\{b\in\mathbb{F}\setminus\mathbb{F}_{2^t}\mid (1+b)^d+b^d\in\mathbb{F}_{2^t}\}| \geqslant 2^t,$$

with equality if and only if R_d has size 2^{t-1} as a set. As a consequence, there exists an element $u\in\mathbb{F}_{2^t}^*$ such that

$$|M_{uc}| \geqslant \sqrt{2^{2t}/(2^t-1)} > 2^{\lfloor t/2\rfloor}.$$

Using the above element uc as b in (2.2), we see that there is some $a\in\mathbb{F}_{2^t}$ such that $W_d(a) > 2^t+2^{\lfloor t/2\rfloor}$ by an averaging argument. The proof of the theorem is now complete. $\square$

Remarks. (1) In the case where $d=1+2^i$, for $x\in\mathbb{F}_{2^t}$, we have $\mathrm{Tr}_m((x+b)^d)=\mathrm{Tr}_t(xv)+\mathrm{Tr}_m(b^d)$, where $v=\mathrm{Tr}_{m/t}(b)^{2^i}+\mathrm{Tr}_{m/t}(b)^{2^{-i}}$. Choosing $b\in\mathbb{F}\setminus\mathbb{F}_{2^t}$ such that $\mathrm{Tr}_{m/t}(b)=1$, we have $v=0$, and $|M_b|=2^t$. We see that Conjecture 1.1 is true in this case by using (2.2).

(2) If d is a Niho exponent, then from [3, p. 253] we know that $2^t|W_d(a)$ for all $a\in\mathbb{F}$. Combining this divisibility result with the conclusion of Theorem 2.1 that there is some $a\in\mathbb{F}$ with $W_d(a)>2^t+2^{\lfloor t/2\rfloor}$, we immediately get $W_d(a)\geqslant 2^{t+1}$. The same argument shows that more generally, for any d, $1\leqslant d\leqslant q-2$, $\gcd(d,q-1)=1$, such that $2^t|W_d(a)$ for all $a\in\mathbb{F}$, Conjecture 1.1 is also true.

3 The Walsh spectrum of $\mathrm{Tr}(x^d)$ with $d=1+2^i+2^{i+t}$

In this section, we assume that $d=1+2^i+2^{i+t}$ for some i, $0<i<t-1$, and $\gcd(d,2^m-1)=1$. Such a d is not a Niho exponent. First, we show that for any d of the aforementioned form, Conjecture 1.1 is true. Secondly, specializing to the $i=1$ case, i.e., $d=3+2^{t+1}$, we determine the Walsh spectrum of $\mathrm{Tr}(x^d)$ completely.

For a nonzero integer n, we use $v_2(n)$ to denote the largest nonnegative integer a such that $2^a|n$.

Lemma 3.1. *Let $m=2t$ and $d=1+2^i+2^{i+t}$ for some i, $0<i<t-1$, with $\gcd(d,2^m-1)=1$. Then $v_2(i+1)\geqslant v_2(t)$.*

Proof. Since $\gcd(d,2^m-1)=1$, we have $\gcd(2^{i+1}+1,2^t-1)=1$. It follows that $\gcd(2^{i+1}-1,2^t-1)$ $=\gcd(2^{2(i+1)}-1,2^t-1)$. Therefore, $\gcd(i+1,t)=\gcd(2(i+1),t)$, which is easily seen to be equivalent to $v_2(i+1)\geqslant v_2(t)$. The proof is complete. □

Let c be a fixed element of $\mathbb{F}^*$ such that $c\neq 1$ and $c^{2^t+1}=1$. Then each element of $\mathbb{F}$ can be written uniquely as $x+yc$ with $x,y\in L:=\mathbb{F}_{2^t}$. We shall write $\bar{c}:=c^{2^t}$, $\theta:=c+\bar{c}$. Now we compute $W_d(a+b\bar{c})$, where $a,b\in L$. For $x,y\in L$, we have

$$\begin{aligned}\mathrm{Tr}((x+yc)^d+(a+b\bar{c})(x+yc)) &= \mathrm{Tr}(x\mathrm{N}_{m/t}(x+yc)^{2^i}+y\mathrm{N}_{m/t}(x+yc)^{2^i}c+ax+by+ayc+bx\bar{c})\\ &= \mathrm{Tr}_t(y(x^2+xy\theta+y^2)^{2^i}\theta)+\mathrm{Tr}_t(ay\theta+bx\theta)\\ &= \mathrm{Tr}_t(yx^{2^{i+1}}\theta+y^{1+2^i}\theta^{1+2^i}x^{2^i})+\mathrm{Tr}_t(y^{1+2^{i+1}}\theta+ay\theta+bx\theta)\\ &= \mathrm{Tr}_t((y^{2^{t-i-1}}\theta^{2^{t-i-1}}+y^{1+2^{t-i}}\theta^{1+2^{t-i}}+b\theta)x)+\mathrm{Tr}_t(y^{1+2^{i+1}}\theta+ay\theta).\end{aligned}$$

Therefore,

$$\begin{aligned}W_d(a+b\bar{c}) &= \sum_{y\in L}\sum_{x\in L}(-1)^{\mathrm{Tr}_t((y^{2^{t-i-1}}\theta^{2^{t-i-1}}+y^{1+2^{t-i}}\theta^{1+2^{t-i}}+b\theta)x)+\mathrm{Tr}_t(y^{1+2^{i+1}}\theta+ay\theta)}\\ &= 2^t\sum_{y}(-1)^{\mathrm{Tr}_t(y^{1+2^{i+1}}\theta+ay\theta)},\end{aligned}$$

where the last sum is taken over

$$\{y\in L\mid y\theta+(y\theta)^{2+2^{i+1}}+(b\theta)^{2^{i+1}}=0\}.$$

After a change of variable, we have

$$W_d(a+b\bar{c})=2^t\sum_{z\in S_b}(-1)^{\mathrm{Tr}_t(z^{1+2^{i+1}}\theta^{-2^{i+1}}+az)},\tag{3.1}$$

where

$$S_b:=\{z\in L\mid z+z^{2+2^{i+1}}+(b\theta)^{2^{i+1}}=0\}.$$

When $b=0$, we have $S_0=\{0,1\}$ since $\gcd(2^{i+1}+1,2^t-1)=1$. It follows that

$$W_d(a)=2^t(1+(-1)^{\mathrm{Tr}_t(\theta^{-1}+a)}),\quad \forall\, a\in L.$$

Choosing $a=\theta^{-1}$, we have $W_d(\theta^{-1})=2^{t+1}$. Thus we have proved the following:

Theorem 3.1. *Conjecture* 1.1 *holds when* d *is of the form* $1+2^i+2^{i+t}$, $0<i<t-1$, *and* $\gcd(d,2^m-1)=1$.

In order to determine the Walsh spectrum of $\mathrm{Tr}(x^d)$, it remains to compute $W_d(a+b\bar{c})$ for those $b\in L^*$. In the case when $b\neq 0$, to compute $W_d(a+b\bar{c})$ using (3.1), we need to solve the equation

$$z+z^{2^{i+1}+2}=w,\quad z\in L,$$

for each $w\in L^*$. For general i, $0<i<t-1$, the solutions are complicated. We will consider the $i=1$ case below.

From now on, we assume that $i=1$ (so $d=3+2^{t+1}$). By Lemma 3.1, $v_2(t)\leqslant 1$; that is, either t is odd or $t\equiv 2 \pmod 4$. The equation we need to consder is now $z^6+z=w$, $z\in L$ and $w\in L^*$.

Assume that $z_0\in L^*$ is a solution to $z^6+z=w$, $w\in L^*$. Suppose z_0+x is another solution with $x\in L^*$. Now expanding $(z_0+x)^6+z_0+x=w$ gives

$$\left(\frac{x}{z_0}\right)^5+\left(\frac{x}{z_0}\right)^3+\left(\frac{x}{z_0}\right)=\frac{1}{z_0^5}.$$

The polynomial $X^5+X^3+X\in\mathbb{F}_2[X]$ is the Dickson polynomial $D_5(X,1)$. For convenience of the reader, we include the definition of the Dickson polynomials here. Let $a\in\mathbb{F}_q$ (here q is an arbitrary prime power) and n be a positive integer. We define the *Dickson polynomial* $D_n(X,a)$ over $\mathbb{F}_q$ by

$$D_n(X,a)=\sum_{j=0}^{\lfloor n/2\rfloor}\frac{n}{n-j}\binom{n-j}{j}(-a)^jX^{n-2j}.$$

It is well known [10] that the Dickson polynomial $D_n(X,a)$, $a\in\mathbb{F}_q^*$, is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(n,q^2-1)=1$. For more details about Dickson polynomials, we refer the reader to [10].

We are now ready to determine the Walsh spectrum of $\mathrm{Tr}(x^d)$ in the case where $m=2t$, t is odd, and $d=3+2^{t+1}$.

Theorem 3.2. *Let* $m=2t$ *be a positive integer with* t *odd, and* $d=3+2^{t+1}$. *The Walsh spectrum of* $\mathrm{Tr}(x^d)$ *over* $\mathbb{F}=\mathbb{F}_{2^m}$ *is given in below.*

$W_d(\cdot)$	Multiplicity
0	$3\cdot 2^{2t-2}$
2^{t+1}	$2^{2t-3}+2^{t-2}$
-2^{t+1}	$2^{2t-3}-2^{t-2}$

Proof. We have observed that $X^5+X^3+X\in\mathbb{F}_2[X]$ is the Dickson polynomial $D_5(X,1)$. If t is odd, then $\gcd(5,2^{2t}-1)=1$; consequently $D_5(X,1)$ induces a permutation of $L=\mathbb{F}_{2^t}$. Hence by the computations that we did above, $|S_b|=0$ or 2 when $b\neq 0$. We also saw that $S_0=\{0,1\}$. It follows that $W_d(a+b\bar{c})$, $a,b\in L$, take three values only: 0, $\pm 2^{t+1}$. Now denote by N_0,N_+,N_- the multiplicity of 0, 2^{t+1}, -2^{t+1} in the Walsh spectrum of $\mathrm{Tr}(x^d)$, respectively. From Lemma 2.1(1), we have

$$N_0+N_++N_-=2^{2t},\quad 2^{t+1}N_+-2^{t+1}N_-=2^{2t},\quad 2^{2t+2}N_++2^{2t+2}N_-=2^{4t}.$$

Solving this system of equations, we get

$$N_0=2^{2t}-2^{2t-2},\quad N_+=2^{2t-3}+2^{t-2},\quad N_-=2^{2t-3}-2^{t-2}.\qquad\square$$

Remarks. (1) Let t be an odd positive integer. The fact that $z^6+z=w$, $w\in\mathbb{F}_{2^t}$, has 0 or 2 solutions in L is equivalent to the fact that $D(6)=\{(1,x,x^6)\mid x\in\mathbb{F}_{2^t}\}\cup\{(0,1,0),(0,0,1)\}$ is a hyperoval in $PG(2,2^t)$. See [5] for more details.

(2) Theorem 3.2 was first proved in [4] by a slightly different argument.

Next, we consider the case where $d = 3 + 2^{t+1}$ and $t \equiv 2 \pmod 4$.

Theorem 3.3. *Let $m = 2t$ be a positive integer with $v_2(t) = 1$, $t \geqslant 6$, and $d = 3 + 2^{t+1}$. The Walsh spectrum of $\mathrm{Tr}(x^d)$ over $\mathbb{F} = \mathbb{F}_{2^m}$ is given in below.*

$W_d(\cdot)$	Multiplicity
0	$2^{2t-1} - 2^{2t-5} - 2^{t-1} + 2^{t-3}$
2^t	$\frac{2^{2t}+2^t}{5}$
-2^t	$\frac{2^{2t}+2^t}{5}$
2^{t+1}	$2^{2t-4} + 2^{t-2}$
-2^{t+1}	$2^{2t-4} - 2^{t-2}$
2^{t+2}	$\frac{2^{2t-6}-2^{t-4}}{5}$
-2^{t+2}	$\frac{2^{2t-6}-2^{t-4}}{5}$

Remarks. The webpage of Philippe Langevin (http://langevin.univ-tln.fr/project/spectrum/) contains very useful data on the Walsh spectrums of the power functions $\mathrm{Tr}(x^d)$ over $\mathbb{F}_{2^m}$, for all integers $m < 26$, and all invertible (modulo $2^m - 1$) exponents d.

The remaining part of this paper is devoted to the proof of Theorem 3.3. From now on, we always assume that $v_2(t) = 1$ and $t \geqslant 6$. Let

$$G := \{x \in \mathbb{F} \mid x^{2^t+1} = 1\}.$$

Furthermore, we will assume that the element c used in (3.1) to have order 5. Since $t \equiv 2 \pmod 4$ by assumption, we have $5 \mid (2^t + 1)$. Thus $c^{2^t+1} = 1$, i.e., $c \in G$ (and $c \notin L$).

Lemma 3.2. *Let $w \in L^*$. Then the number of solutions $z \in L$ to*

$$z^6 + z = w$$

is 0, 1, 2 or 6.

Proof. The main difference from the t odd case is that $X^5 + X^3 + X \in \mathbb{F}_2[X]$ no longer induces a permutation of $L = \mathbb{F}_{2^t}$ when $t \equiv 2 \pmod 4$. We start in the same way as before. Assume that $z_0 \in L^*$ is a solution to $z^6 + z = w$, $w \in L^*$. Suppose $z_0 + x$ is another solution with $x \in L^*$. Then expanding

$$(z_0 + x)^6 + z_0 + x = w$$

gives

$$\left(\frac{x}{z_0}\right)^5 + \left(\frac{x}{z_0}\right)^3 + \left(\frac{x}{z_0}\right) = \frac{1}{z_0^5}. \tag{3.2}$$

The above equation has 0, 1, or 5 solutions in L when $v_2(t) = 1$ and $t \geqslant 6$. This can be seen as follows.

It is well known that each element y of L^* can be written in the form $u + \frac{1}{u}$, with $u \in L^*$ or $u \in G$, according as $\mathrm{Tr}_t(1/y)$ is equal to 0 or 1 (see [10]). Now if $x = z_0(u + \frac{1}{u}) \in L$ is a solution to (3.2), then so are $z_0(\gamma u + \frac{1}{\gamma u})$, $\gamma \in \mathbb{F}^*$ and $\gamma^5 = 1$, since

$$D_5\left(\gamma u + \frac{1}{\gamma u}, 1\right) = (\gamma u)^5 + \frac{1}{(\gamma u)^5} = u^5 + \frac{1}{u^5}.$$

When $u \in L^*$, $\gamma u + \frac{1}{\gamma u}$ is in L if and only if $\gamma = 1$. When $u \in G$, any choice of γ ($\gamma^5 = 1$) will give $\gamma x + \frac{1}{\gamma x} \in L$. This proves the claim that (3.2) has 0, 1 or 5 solutions in L. The conclusion of the lemma follows as a consequence. $\square$

From Lemma 3.2 and (3.1), we see that the Walsh coefficients of $\mathrm{Tr}(x^{3+2^{t+1}})$ are in $\{\pm i \cdot 2^t \mid i = 0, 1, 2, 4, 6\}$. We use N_i to denote the number of $a + b\bar{c} \in \mathbb{F}$ such that $W_d(a + b\bar{c}) = i \cdot 2^t$, for $i \in \{0, \pm1, \pm2, \pm4, \pm6\}$.

3.1 The equation $z^6 + z = w$, $w \in L^*$

Now, we examine for which $w \in L^*$, $z^6+z=w$, has six solutions in L. Assume that z_0 and x are as in the proof of Lemma 3.2. By the above analysis, there exists $u \in G$ such that $\frac{x}{z_0} = u + \frac{1}{u}$, and $\frac{1}{z_0^5} = u^5 + \frac{1}{u^5}$, i.e., $z_0^5 = \frac{1}{u^{-5}+u^5}$. Since $\gcd(5, 2^t-1) = 1$, we get $z_0 = \frac{1}{(u^{-5}+u^5)^{1/5}}$. The other five solutions are

$$\frac{1}{(u^{-5}+u^5)^{1/5}}\left(1 + u\gamma + \frac{1}{u\gamma}\right), \quad \gamma^5 = 1.$$

Therefore, $z^6 + z = w$, $w \in L^*$, has six solutions in L if and only if w is in the following set

$$T_6 := \left\{ z^6 + z \;\middle|\; z = \frac{1}{(u^{-5}+u^5)^{1/5}},\, u \in G,\, u^5 \neq 1 \right\}.$$

The set T_6 has size $\frac{2^t+1-5}{5\cdot 2\cdot 6} = \frac{2^{t-2}-1}{15}$, the factor 5 in the denominator comes from the fact that $u \mapsto u^5$ is 5-to-1 on G; the factor 6 comes from the fact that $z \mapsto z^6 + z$ is 6-to-1 on the set in consideration; and the factor 2 comes from the fact that u and u^{-1} give the same element. In this case, with $(b\theta)^4 = w$, $W_d(a + b\bar{c}) \in \{\pm i \cdot 2^t \mid i = 0, 2, 4, 6\}$.

Next, we examine for which $w \in L$, $z^6 + z = w$ has two solutions in L. Clearly, when $w = 0$, this equation has two solutions in L. So in what follows we consider the case where $w \neq 0$. Assume that z_0 and x are as in the proof of Lemma 3.2. By the same analysis, there exists $u \in L^*$ such that $\frac{x}{z_0} = u + \frac{1}{u}$, and $\frac{1}{z_0^5} = u^5 + \frac{1}{u^5}$, i.e., $z_0^5 = \frac{1}{u^{-5}+u^5}$. Therefore, $z^6 + z = w$, $w \in L$, has two solutions in L if and only if w is in the following set

$$T_2 := \left\{ z^6 + z \;\middle|\; z = \frac{1}{(u^{-5}+u^5)^{1/5}},\, u \in L \setminus \mathbb{F}_4 \right\} \cup \{0\}.$$

The set T_2 has size $\frac{2^t-4}{2\cdot 2} + 1 = 2^{t-2}$. In this case, with $(b\theta)^4 = w$, $W_d(a + b\bar{c}) \in \{\pm i \cdot 2^t : i = 0, 2\}$.

It now follows that there are $2^t - 2\cdot 2^{t-2} - 6 \cdot \frac{2^t-4}{60} = \frac{2^{t+1}+2}{5}$ elements $w \in L$ such that $z^6 + z = w$ has only one solution in L. Only these w will give the values $W_d(a + b\bar{c}) = \pm 2^t$ (again with $(b\theta)^4 = w$). We observe that the two values, 2^t and -2^t, occur for equally many $a \in L$, since for the unique solution $z_0 \in L^*$ to $z^6 + z = w$, half of the a's in L satisfy $\mathrm{Tr}_t(az_0) = 0$ and the other half satisfy $\mathrm{Tr}_t(az_0) = 1$. Therefore, we have

$$N_1 = N_{-1} = 2^{t-1} \cdot \frac{2^{t+1}+2}{5} = \frac{2^{2t}+2^t}{5}.$$

Finally, we note that the number of $w \in L$ such that $z^6 + z = w$ has no solutions in L at all is equal to $2^t - \frac{2^{t-2}-1}{15} - 2^{t-2} - \frac{2^{t+1}+2}{5} = \frac{2^t-1}{3}$.

3.2 $N_6 = N_{-6} = 0$

We now show that $W_d(a + b\bar{c}) \neq \pm 6 \cdot 2^t$ for all $a, b \in L$. As seen above, only when $z^6 + z = w$, $w = (b\theta)^4 \in L^*$, has 6 solutions in L, could $W_d(a + b\bar{c})$ possibly be equal to $\pm 6 \cdot 2^t$. Let $z_0 = \frac{1}{(u^{-5}+u^5)^{1/5}} \in L^*$, $u \in G$, be a solution to $z^6 + z = w$, $w = (b\theta)^4 \in L^*$. The other five solutions are $z_j = z_0 + x_j \in L$, with $\frac{x_j}{z_0} = u\gamma^j + \frac{1}{u\gamma^j}$, $1 \leqslant j \leqslant 5$, $o(\gamma) = 5$, $u \in G$. The fact that $\pm 6 \cdot 2^t$ won't occur as Walsh coefficients of $\mathrm{Tr}(x^d)$ amounts to the fact that the following system of equations does not have a solution $a \in L$:

$$\mathrm{Tr}_t(z_j^5\theta^{-4} + az_j) = \mathrm{Tr}_t(z_0^5\theta^{-4} + az_0), \quad 1 \leqslant j \leqslant 5.$$

We will prove the latter fact by way of contradiction. Assume that the above system has a solution $a \in L$. With $z_j = x_j + z_0$, we get

$$\mathrm{Tr}_t(x_j(z_0^4\theta^{-4} + z_0^{2^{t-2}}\theta^{-1} + a)) = \mathrm{Tr}_t(x_j^5\theta^{-4}), \quad 1 \leqslant j \leqslant 5.$$

Since $\frac{x_j}{z_0} = u\gamma^j + \frac{1}{u\gamma^j} = \mathrm{Tr}_{m/t}(u\gamma^j)$, we have

$$\mathrm{Tr}_m(u\gamma^j z_0(z_0^4\theta^{-4} + z_0^{2^{t-2}}\theta^{-1} + a)) = \mathrm{Tr}_m((u^5 + u^3\gamma^{3j})z_0^5\theta^{-4}), \quad 1 \leqslant j \leqslant 5.$$

Now, we rewrite the above equations as

$$\mathrm{Tr}_4(\gamma^j U) = V + \mathrm{Tr}_4(\gamma^{3j} W), \quad 1 \leqslant j \leqslant 5,$$

where

$$\begin{aligned} U &:= \mathrm{Tr}_{m/4}(uz_0(z_0^4\theta^{-4} + z_0^{2^{t-2}}\theta^{-1} + a)) = \mathrm{Tr}_{m/4}\left(\frac{u}{u^5+u^{-5}}\theta^{-4} + \frac{u}{(u^5+u^{-5})^{1/4}}\theta^{-1} + uz_0 a\right), \\ V &:= \mathrm{Tr}_m(u^5 z_0^5 \theta^{-4}) = \mathrm{Tr}_m\left(\frac{u^5}{u^5+u^{-5}}\theta^{-4}\right) = \mathrm{Tr}_t(\theta^{-1}), \\ W &:= \mathrm{Tr}_{m/4}(u^3 z_0^5 \theta^{-4}) = \mathrm{Tr}_{m/4}\left(\frac{u^3}{u^5+u^{-5}}\theta^{-4}\right). \end{aligned}$$

Taking summation of the above equations over $1 \leqslant j \leqslant 5$, we get $V = 0$. However, as we stated before, $\mathrm{Tr}_t(\theta^{-1}) = 1$ since $\theta = c + c^{-1}$ with $c \in G$. This contradiction completes the proof.

3.3 N_4 and N_{-4}

(1) We now compute N_4 and N_{-4}. As we have seen above, $W_d(a + b\bar{c}) = \pm 2^{t+2}$ if and only if $z^6 + z = w$, $w = (b\theta)^4 \in L^*$, has 6 solutions in L, and for some $i_0 \in \{0, 1, \dots, 5\}$ the following equations hold:

$$\mathrm{Tr}_t(z_j^5\theta^{-4} + az_j) = \mathrm{Tr}_t(z_{i_0}^5\theta^{-4} + az_{i_0}) + 1, \quad 0 \leqslant j \leqslant 5, \quad j \neq i_0.$$

Without loss of generality, we may assume that $i_0 = 0$. Similar to the above computations, we can rewrite the above equations as

$$\mathrm{Tr}_4(\gamma^j U) = \mathrm{Tr}_4(\gamma^{3j} W), \quad 1 \leqslant j \leqslant 5,$$

where U, W are the same as above. It follows that

$$\mathrm{Tr}_4(\gamma^j U) = \mathrm{Tr}_4(\gamma^j W^2), \quad 1 \leqslant j \leqslant 5.$$

Since γ^j, $1 \leqslant j \leqslant 5$, span $\mathbb{F}_{2^4}$, we obtain that $U = W^2$, i.e.,

$$\begin{aligned} \mathrm{Tr}_{m/4}(uz_0 a) &= \mathrm{Tr}_{m/4}\left(\frac{u}{(u^5+u^{-5})^{1/5}}a\right) \\ &= \mathrm{Tr}_{m/4}\left(\frac{u}{u^5+u^{-5}}\theta^{-4} + \frac{u}{(u^5+u^{-5})^{1/4}}\theta^{-1} + \frac{u^6}{u^{10}+u^{-10}}\theta^{-8}\right). \end{aligned}$$

Since the element c has (multiplicative) order 5, it follows that $\theta = c + \bar{c}$ has order 3. We have

$$\begin{aligned} \mathrm{Tr}_{m/4}(uz_0 a) &= \mathrm{Tr}_{m/4}\left(\frac{u}{u^5+u^{-5}}\theta^2 + \frac{u}{(u^5+u^{-5})^{1/4}}\theta^2 + \frac{u^6}{u^{10}+u^{-10}}(\theta^2+1)\right) \\ &= \theta^2\,\mathrm{Tr}_{m/4}\left(\frac{u}{u^5+u^{-5}} + \frac{u^{16}}{u^{20}+u^{-20}} + \frac{u^6}{u^{10}+u^{-10}}\right) + \mathrm{Tr}_{m/4}\left(\frac{u^6}{u^{10}+u^{-10}}\right) \\ &= \theta^2\,\mathrm{Tr}_{m/4}\left(\frac{u}{u^5+u^{-5}} + \frac{u^{-4}}{u^{20}+u^{-20}}\right) + \mathrm{Tr}_{m/4}\left(\frac{u^3}{u^5+u^{-5}}\right)^2 \\ &= \theta^2\,\mathrm{Tr}_{m/4}\left(\frac{u+u^{-1}}{u^5+u^{-5}}\right) + \theta^2\,\mathrm{Tr}_{m/2}\left(\frac{u^{-1}}{u^5+u^{-5}}\right) + \mathrm{Tr}_{m/4}\left(\frac{u^3}{u^5+u^{-5}}\right)^2 \\ &= \theta^2\,\mathrm{Tr}_{t/2}\left(\frac{u+u^{-1}}{u^5+u^{-5}}\right) + \theta^2\,\mathrm{Tr}_{t/2}\left(\frac{u+u^{-1}}{u^5+u^{-5}}\right) + \mathrm{Tr}_{m/4}\left(\frac{u^3}{u^5+u^{-5}}\right)^2 \\ &= \mathrm{Tr}_{m/4}\left(\frac{u^3}{u^5+u^{-5}}\right)^2. \end{aligned}$$

Conversely, if $\mathrm{Tr}_{m/4}(uz_0 a) = \mathrm{Tr}_{m/4}(\frac{u^3}{u^5+u^{-5}})^2$, $a \in L$, and $z^6 + z = w$, $w = (b\theta)^4 \in L^*$, has 6 solutions in L, then $W_d(a + b\bar{c}) = \pm 2^{t+2}$.

Below we will count the number of solutions to

$$\mathrm{Tr}_{m/4}(uz_0a) = \mathrm{Tr}_{m/4}\left(\frac{u^3}{u^5+u^{-5}}\right)^2, \quad a \in L. \tag{3.3}$$

Write $\mathrm{Tr}_{m/4}(\frac{u^3}{u^5+u^{-5}})^2 = h + g\gamma$ with $h, g \in \mathbb{F}_{2^2}$ and

$$uz_0 = \frac{u}{(u^5+u^{-5})^{1/5}} = \alpha + \beta\gamma, \quad \alpha, \beta \in L = \mathbb{F}_{2^t}, \quad o(\gamma) = 5.$$

We claim that $\alpha/\beta \notin \mathbb{F}_4^*$. Otherwise, u is in $\mathbb{F}_{2^4}^* \cdot \mathbb{F}_{2^t}^*$ and thus has order dividing $\mathrm{lcm}(15, 2^t-1) = 5(2^t-1)$. Noting that u has order dividing 2^t+1, we have $u^5 = 1$, which is a contradiction. Now (3.3) becomes $\mathrm{Tr}_{m/4}(\alpha a) + \mathrm{Tr}_{m/4}(\beta a)\gamma = h + g\gamma$, that is,

$$\mathrm{Tr}_{t/2}(\alpha a) = h, \quad \mathrm{Tr}_{t/2}(\beta a) = g.$$

Since $\alpha/\beta \notin \mathbb{F}_4^*$, this system of equations clearly has 2^{t-4} solutions $a \in L$.

We thus have

$$N_4 + N_{-4} = 6 \cdot 2^{t-4} \cdot \frac{2^{t-2}-1}{15} = \frac{2^{2t-5}-2^{t-3}}{5}.$$

(2) Let $b \in L^*$ be such that $z^6 + z = w$, $w = (b\theta)^4 \in L^*$, has 6 solutions in L. Assume that the six solutions are z_j, $0 \leqslant j \leqslant 5$, as given above. We claim that for each $i_0 \in \{0, 1, \ldots, 5\}$ there exists an $x \in L$ such that

$$\mathrm{Tr}_{m/4}(uz_{i_0}x) = 0, \quad \mathrm{Tr}_t(z_jx) = 1, \quad \forall\, j, \quad 0 \leqslant j \leqslant 5. \tag{3.4}$$

An immediate consequence is that $N_4 = N_{-4}$; this can be seen as follows: If $W_d(a + b\bar{c}) = 4 \cdot 2^t$, $a, b \in L$, then $W_d(x + a + b\bar{c}) = -4 \cdot 2^t$ since every term in the sum on the right-hand side of (3.1) is negated and $\mathrm{Tr}_{m/4}(uz_{i_0}(x+a)) = \mathrm{Tr}_{m/4}(uz_{i_0}a) = \mathrm{Tr}_{m/4}(\frac{u^3}{u^5+u^{-5}})^2$. We thus conclude that

$$N_4 = N_{-4} = \frac{2^{2t-6}-2^{t-4}}{5}.$$

Now we prove the claim about the existence of solution to (3.4). Again, without loss of generality, we assume that $i_0 = 0$. Multiplying both sides of $\mathrm{Tr}_{m/4}(uz_0x) = 0$ by γ^j and taking trace to $\mathbb{F}_2$, we get

$$\mathrm{Tr}_t(x_jx) = 0, \quad \forall\, 1 \leqslant j \leqslant 5.$$

As above, writing $uz_0 = \alpha + \beta\gamma$, $\alpha, \beta \in L$, $o(\gamma) = 5$, and noting that $z_j = x_j + z_0$, for $1 \leqslant j \leqslant 5$, we see that the system of equations under consideration reduces to

$$\mathrm{Tr}_{t/2}(\alpha x) = 0, \quad \mathrm{Tr}_{t/2}(\beta x) = 0, \quad \mathrm{Tr}_t(z_0x) = 1.$$

We prove that this system of equations has a solution by showing that z_0 does not lie in the $\mathbb{F}_4$-linear span of α and β. Raising $uz_0 = \alpha + \beta\gamma$ to the 2^t-th power gives $u^{-1}z_0 = \alpha + \beta\gamma^{-1}$. We solve that

$$\alpha = \frac{u\gamma^{-1} + u^{-1}\gamma}{\gamma + \gamma^{-1}} z_0, \quad \beta = \frac{u + u^{-1}}{\gamma + \gamma^{-1}} z_0.$$

Suppose to the contrary that there exist $r, s \in \mathbb{F}_4$ such that $r\alpha + s\beta = z_0$. After expansion we get

$$u^2(r + s\gamma^{-1}) + u(\gamma + \gamma^{-1}) + (r + s\gamma) = 0.$$

This is a degree 2 equation with coefficients in $\mathbb{F}_{2^4}$. Since $u \in \mathbb{F}_{2^{2t}}$ and $2||t$, we have $u \in \mathbb{F}_{16}^*$. Hence $u^5 = 1$, which is impossible.

3.4 N_2, N_{-2} and N_0

It remains to determine N_0, N_2, N_{-2}. By Lemma 2.1, we have the following equations:

$$\begin{aligned}
&N_0 + N_2 + N_{-2} = 2^{2t} - \frac{2^{2t-5} - 2^{t-3}}{5} - 2 \cdot \frac{2^{2t} + 2^t}{5} = 19 \cdot 2^{2t-5} - 3 \cdot 2^{t-3}, \\
&2^{t+1}(N_2 - N_{-2}) = 2^{2t}, \\
&2^{2t+2}(N_2 + N_{-2}) = 2^{4t} - \frac{2^{2t-5} - 2^{t-3}}{5} \cdot 2^{2t+4} - 2 \cdot \frac{2^{2t} + 2^t}{5} \cdot 2^{2t} = 2^{4t-1}.
\end{aligned}$$

Solving these equations, we get

$$N_0 = 2^{2t-1} - 2^{2t-5} - 2^{t-1} + 2^{t-3}, \quad N_2 = 2^{2t-4} + 2^{t-2}, \quad N_{-2} = 2^{2t-4} - 2^{t-2}.$$

The proof of Theorem 3.3 is now complete. □

Acknowledgements The research of Tao Feng was supported in part by Fundamental Research Fund for the Central Universities of China, Zhejiang Provincial Natural Science Foundation (Grant No. LQ12A01019), National Natural Science Foundation of China (Grant No. 11201418) and Research Fund for Doctoral Programs from the Ministry of Education of China (Grant No. 20120101120089). The research of Ka Hin Leung was supported in part by AcRF grant (Grant No. R-146-000-158-112).

References

1 Aubry Y, Langevin P. On a conjecture of Helleseth. ArXiv:1212.6553v1
2 Canteaut A, Charpin P, Dobbertin H. Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. IEEE Trans Inform Theory, 2000, 46: 4–8
3 Charpin P. Cyclic codes with few weights and Niho exponents. J Combin Theory Ser A, 2004, 108: 247–259
4 Cusick T, Dobbertin H. Some new three-valued crosscorrelation functions for binary m-sequences. IEEE Trans Inform Theory, 1996, 42: 1238–1240
5 Evans R, Hollmann H D L, Krattenthaler C, et al. Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets. J Combin Theory Ser A, 1999, 87: 74–119
6 Feng T. On cyclic codes of length $2^{2^r} - 1$ with two zeros whose dual codes have three weights. Des Codes Cryptogr, 2012, 62: 253–258
7 Helleseth T. Some results about the cross-correlation function between two maximal linear sequences. Discrete Math, 1976, 16: 209–232
8 Hollmann H D L, Xiang Q. A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences. Finite Fields Appl, 2001, 7: 253–286
9 Katz D. Weil sums of binomials, three-level correlation, and a conjecture of Helleseth. J Combin Theory Ser A, 2012, 119: 1644–1659
10 Lidl R, Mullen G L, Turnwald G. Dickson Polynomials. Harlow: Longman Scientific and Technical, 1993
11 Niho Y. Multivalued cross-correlation functions between two maximal linear recursive sequences. PhD dissertation. Los Angeles: University of Southern California, 1972